UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/627,019 | 07/25/2003 | Bhavna Bhatnagar | 03226/503001; P8951 | 3673 |

32615 7590 06/04/2008

OSHA LIANG L.L.P./SUN
1221 MCKINNEY, SUITE 2800
HOUSTON, TX 77010

| EXAMINER | |
|---|---|
| LANIER, BENJAMIN E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 06/04/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lord@oshaliang.com
DOCKETING@OSHALIANG.COM
hathaway@oshaliang.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/627,019 | BHATNAGAR ET AL. | |
| | Examiner | Art Unit | |
| | BENJAMIN E. LANIER | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *25 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3,8,11-15,17-19,22 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,8,11-15,17-19,22 and 23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

2. Applicant argues, "Modifying Narin by combining the trusted entity (i.e., the identity servers) with the trusting entity (i.e., the DRM servers) changes the basic principle of operation which requires a one way trust relationship between the two necessarily different servers." This argument is not persuasive because implementing the functionality of two servers on a single server in no way changes the principle operation of Narin. The principle operation of Narin is not to generate a one way trust relationship between the identity and DRM servers. Instead the principle operation is provide rights management for content by providing trust models between different **domains**, not the identity server and DRM server within each domain.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1-3, 8, 11-15, 17-19, 22, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narin, U.S. Publication No. 2004/0003251, in view of Tanaka, U.S. Publication No. 2001/0027440. Referring to claim 1, Narin discloses a domain-based trust establishment model wherein two corporation servers (Figure 11) establish a trust relationship ([0096]) by receiving and storing the public key certificates ([0104]) of the other corporation server in their trusted identity server lists (Figure 11 & [0097]), which meets the limitations of receiving a first certificate of a first server by a second server, storing said first certificate of said first server in a first trusted partner list accessible by said second server, receiving a second certificate of said second server by said first server, and storing said second certificate of said second server in a second trusted partner list accessible by said first server. This allows employees from company B to access content from company A, and visa versa, by submitting a request for content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of wherein access by a client to a resource associated with said first server is controlled as a function of said first trusted partner list. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time

the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 2, Narin discloses that regardless of which server contains the content, each user contacts the server in their own department to obtain a license to access the content ([0114]), which meets the limitation of determining an identity of said second server as a function of said authentication assertion reference. The user submits a license request, containing the identity certificate, to the DRM server ([0117]), which meets the limitation of initiating use of said resource by said client, wherein an authentication assertion reference is provided by said client, sending an authentication request containing said first certificate of said first server to said second server. The DRM server determines whether the identity certificate was issued by a identity server in the trusted domain ([0117]), which meets the limitation of determining if said first certificate is contained in said first trusted partner list of said second server. If the identity certificate is in the trusted domain, a license is granted to the requestor (Figure 5A, 618), which meets the limitation of sending an authentication assertion indicating that the client has been authenticated from said second server to said first server when said first certificate is contained in said first trusted partner list of said second server. If the identity certificate is not in the trusted domain, then the license request is rejected ([0117] & Figure 5A, 614), which meets the limitation of sending an authentication assertion, indicating that said client has not been authenticated, from said second server to said first server when said first certificate is not contained in said first trusted partner list of said second server. This allows employees from company B to access content from company A, and visa versa, by submitting a request for

content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of providing said resource to said client by said first server when said authentication assertion indicates that said client has been authenticated. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 3, Narin discloses that the clients login to the servers with a user-id and password scheme ([0058]), which meets the limitation of logging-on to said second server by said client, and authenticating said client by said second server. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 8, Narin discloses a domain-based trust establishment model wherein two corporation servers (Figure 11) establish a trust relationship ([0096]) by receiving and

storing the public key certificates ([0104]) of the other corporation server in their trusted identity server lists (Figure 11 & [0097]). Regardless of which server contains the content, each user contacts the server in their own department to obtain a license to access the content ([0114]), which meets the limitation of determining an identity said issuing server as a function of said authentication assertion reference. The user submits a license request, containing the identity certificate, to the DRM server ([0117]), which meets the limitation of initiating use of a resource associated with a relying server by a client, wherein an authentication assertion reference is provided by said client to said relying server, and wherein said authentication assertion reference is provided to said client by an issuing server. The DRM server determines whether the identity certificate was issued by a identity server in the trusted domain ([0117]), which meets the limitation of determining if said certificate is contained in a trusted partner list of said issuing server. If the identity certificate is in the trusted domain, a license is granted to the requestor (Figure 5A, 618), which meets the limitation of sending an authentication assertion indicating that the client has been authenticated from said issuing server to said relying server when said certificate is contained in said trusted partner list of said issuing server. If the identity certificate is not in the trusted domain, then the license request is rejected ([0117] & Figure 5A, 614), which meets the limitation of sending an authentication assertion, indicating that said client has not been authenticated, from said issuing server to said relying server when said certificate is not contained in said trusted partner list of said issuing server. This allows employees from company B to access content from company A, and visa versa, by submitting a request for content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received

public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of providing said resource to said client by said relying server when said authentication assertion indicates that said client has been authenticated. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 11, Narin discloses that the clients login to the servers with a user-id and password scheme ([0058]), which meets the limitation of logging-on to said issuing server by said client, and authenticating said client by said issuing server. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 12, Narin discloses a domain-based trust establishment model wherein two corporation servers (Figure 11) establish a trust relationship ([0096]) by receiving and storing the public key certificates ([0104]) of the other corporation server in their trusted identity server lists (Figure 11 & [0097]), which meets the limitations of a first server, a first

administration module, a first trusted partner list communicatively coupled to said first administration module, a second server, a second administration module, a second trusted partner list communicatively coupled to said second administration module. This allows employees from company B to access content from company A, and visa versa, by submitting a request for content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of wherein access by a client to a resource associated with said first server is controlled as a function of said first trusted partner list. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claims 13-15, Narin discloses that this allows employees from company B to access content from company A, and visa versa, by submitting a request for content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of said first administration module receives a credential of said second server, said first administration module stores said credential of said second server in

said first trusted partner list, said credential comprises a certificate. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 17, Narin discloses a domain-based trust establishment model wherein two corporation servers (Figure 11) establish a trust relationship ([0096]) by receiving and storing the public key certificates ([0104]) of the other corporation server in their trusted identity server lists (Figure 11 & [0097]). This allows employees from company B to access content from company A, and visa versa, by submitting a request for content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of said client, said first server communicatively coupled to said client and said second server, wherein said first server further comprises a first session module, a first authentication module, and said second server communicatively coupled to said client and said first server, wherein said second server further comprises, a second session module, and a second authentication module. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of

ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claims 18, 19, 22, Narin discloses that this allows employees from company B to access content from company A, and visa versa, by submitting a request for content access along with the employee's identity certificate, which includes the company's public key certificate, to the other company's DRM server such that the DRM server compares the received public key certificate with the public key certificates stored in the trusted identity server list ([0095] & [0098]), which meets the limitation of said second session module determines an identity of said first server as a function of an authentication assertion reference received from said client, said first session module determines a trusted status of said second server as a function of a certificate received from said second session module, said first session module provides for secure transfer of information for authenticating said client. Narin does not disclose that the identity server and DRM server are implemented in a single server configuration. Tanaka discloses multiple servers being implemented in a single server configuration ([0162]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the identity server and DRM server for each respective corporation to be implemented on a single server in order to reduce the cost and overhead for the corporation by reducing the number of servers.

Referring to claim 23, Narin discloses utilizing the SOAP environment for communications ([0051]), which meets the limitation of said first session module generates and processes SAML request and assertions contained in SOAP envelopes.

***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132